UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/658,310	09/09/2003	Ed H. Frank	14177US02	2145

23446 7590 03/15/2011

MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661

EXAMINER	
JOHNSON, CARLTON	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
03/15/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/658,310
Filing Date: September 09, 2003
Appellant(s): FRANK ET AL.

Frankie W. Wong Registration No. 61,832
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed January 4, 2011 appealing from the Office action mailed July 28, 2010.

(1) Real Party in Interest

The examiner has no comment on the statement, or lack of statement, identifying by name the real party in interest in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The following is a list of claims that are rejected and pending in the application:

Listing of claims:

1. (Previously presented) A method for multiple encryption in a multi- band multi-protocol hybrid wired/wireless network, the method comprising:
receiving on a first PHY channel of an access point, a request for initiation of a communication session from an originating access device;
authenticating said communication session by authenticating said originating access device using a second PHY channel; and
hosting said communication session over a third PHY channel, said third PHY channel established between said access point and said originating access device.

2. (Previously presented) The method according to claim 1, comprising generating at least one encryption/decryption key for use during said communication session.

3. (Previously presented) The method according to claim 2, wherein said

authenticating comprises requesting authentication information from an authentication server.

4. (Previously presented) The method according to claim 3, wherein said authenticating comprises delivering at least a portion of said authentication information received from said authentication server to said originating access device via said second PHY channel.

5. (Previously presented) The method according to claim 4, comprising delivering said at least one encryption/decryption key to said originating access device via one of said first PHY channel or said second PHY channel.

6. (Previously presented) The method according to claim 1, comprising receiving an identification of said originating access device by said access point.

7. (Previously presented) The method according to claim 6, wherein said identity of said originating access device is one or more of a WEP key, a MAC address, and/or an IP address.

8. (Previously presented) The method according to claim 1, comprising acknowledging said received request on said first PHY channel.

9. (Previously presented) The method according to claim 1, comprising determining a type of traffic generated by said originating access device on said first PHY channel.

10. (Previously presented) The method according to claim 9, comprising generating at least one encryption/decryption key dependent on said determined traffic type.

11. (Previously presented) The method according to claim 10, comprising distributing said generated at least one encryption/decryption key via one or both of said second PHY channel and/or said third PHY channel.

12. (Previously presented) The method according to claim 1, comprising establishing at least one virtual channel between said originating access device and a terminating access device.

13. (Previously presented) The method according to claim 12, comprises tunneling information between said originating access device and said terminating access device.

14. (Previously presented) The method according to claim 12, comprising establishing at least a portion of said at least one virtual channel over at least a portion

of one of said first PHY channel, said second PHY channel or said third PHY channel.

15. (Previously presented) A machine-readable storage, having stored thereon, a computer program having at least one code section for providing multiple encryption in a multi-band multi-protocol hybrid wired/wireless network, the at least one code section executable by a machine for causing the machine to perform the steps comprising:

receiving on a first PHY channel of an access point, a request for initiation of a communication session from an originating access device;

authenticating said communication session by authenticating said originating access device using a second PHY channel; and

hosting said communication session over a third PHY channel, said third PHY channel established between said access point and said originating access device.

16. (Previously presented) The machine-readable storage according to claim 15, comprising code for generating at least one encryption/decryption key for use during said communication session.

17. (Previously presented) The machine-readable storage according to claim 16, wherein authenticating code comprises code for requesting authentication information from an authentication server.

18. (Previously presented) The machine-readable storage according to claim 17, comprising code for delivering at least a portion of said authentication information received from said authentication server to said originating access device via said second PHY channel.

19. (Previously presented) The machine-readable storage according to claim 18, comprising code for delivering said at least one encryption/decryption key to said originating access device via one of said first PHY channel or said second PHY channel.

20. (Previously presented) The machine-readable storage according to claim 15, comprising code for receiving an identification of said originating access device by said access point.

21. (Previously presented) The machine-readable storage according to claim 20, wherein said identity of said originating access device is one or more of a WEP key, a MAC address, and/or an IP address.

22. (Previously presented) The machine-readable storage according to claim 15, comprising code for acknowledging said received request on said first PHY channel.

23. (Previously presented) The machine-readable storage according to claim 15, comprising code for determining a type of traffic generated by said originating access

device on said first PHY channel.

24. (Previously presented) The machine-readable storage according to claim 23, comprising code for generating at least one encryption/decryption key dependent on said determined traffic type.

25. (Previously presented) The machine-readable storage according to claim 24, comprising code for distributing said generated at least one encryption/decryption key via one or both of said second PHY channel and/or said third PHY channel.

26. (Previously presented) The machine-readable storage according to claim 15, comprising code for establishing at least one virtual channel between said originating access device and a terminating access device.

27. (Previously presented) The machine-readable storage according to claim 26, comprises code for tunneling information between said originating access device and said terminating access device.

28. (Previously presented) The machine-readable storage according to claim 26, comprising code for establishing at least a portion of said at least one virtual channel over at least a portion of one of said first PHY channel, said second PHY channel or said third PHY channel.

29. (Previously presented) A system for multiple encryption in a multi- band multi-protocol hybrid wired/wireless network, the system comprising:

at least one receiver of an access point adapted to receive on a first PHY channel, a request for initiation of a communication session from an originating access device;

at least one authenticator adapted to authenticate said communication session by authenticating said originating access device using a second PHY channel; and

a third PHY channel being adapted to facilitate hosting of said communication session, said third PHY channel established between said access point and said originating access device.

30. (Previously presented) The system according to claim 29, wherein said at least one authenticator is adapted to generate at least one encryption/decryption key for use during said communication session.

31. (Previously presented) The system according to claim 30, wherein said at least one authenticator is adapted to receive requests for authentication information.

32. (Previously presented) The system according to claim 31, wherein said authenticator is adapted to deliver at least a portion of said authentication information received from said authentication server to said originating access device via said

second PHY channel.

33. (Previously presented) The system according to claim 32, wherein said at least one authenticator is adapted to deliver said at least one encryption/decryption key to said originating access device via one of said first PHY channel or said second PHY channel.

34. (Previously presented) The system according to claim 29, wherein said at least one receiver is adapted to receive an identification of said originating access device by said access point.

35. (Previously presented) The system according to claim 34, wherein said identity of said originating access device is one or more of a WEP key, a MAC address, and/or an IP address.

36. (Previously presented) The system according to claim 29, wherein said at least one receiver is adapted to acknowledge said received request on said first PHY channel.

37. (Previously presented)The system according to claim 29, wherein said at least one authenticator is adapted to determine a type of traffic generated by said originating access device on said first PHY channel.

38. (Previously presented)The system according to claim 37, wherein said at least one authenticator is adapted to generate at least one encryption/decryption key dependent on said determined traffic type.

39. (Previously presented) The system according to claim 38, wherein said at least one authenticator is adapted to distribute said generated at least one encryption/decryption key via one or both of said second PHY channel and/or said third PHY channel.

40. (Previously presented)The system according to claim 29, wherein said at least one receiver is adapted to establish at least one virtual channel between said originating access device and a terminating access device.

41. (Previously presented)The system according to claim 40, wherein said at least one receiver is adapted to tunnel information between said originating access device and said terminating access device.

42. (Previously presented) The system according to claim 40, wherein said at least one receiver is adapted to establish at least a portion of said at least one virtual channel over at least a portion of one of said first PHY channel, said second PHY channel or said third PHY channel.

(4) Status of Amendments After Final

The examiner has no comment on the appellant's statement of the status of amendments after final rejection contained in the brief.

(5) Summary of Claimed Subject Matter

The examiner has no comment on the summary of claimed subject matter contained in the brief.

(6) Grounds of Rejection to be Reviewed on Appeal

The examiner has no comment on the appellant's statement of the grounds of rejection to be reviewed on appeal. Every ground of rejection set forth in the Office action from which the appeal is taken (as modified by any advisory actions) is being maintained by the examiner except for the grounds of rejection (if any) listed under the subheading "WITHDRAWN REJECTIONS." New grounds of rejection (if any) are provided under the subheading "NEW GROUNDS OF REJECTION."

(7) Claims Appendix

The examiner has no comment on the copy of the appealed claims contained in the Appendix to the appellant's brief.

(8) Evidence Relied Upon

7,039,027	Bridgelall	12-2001
6,088,451	He	6-1996
7,325,058	Sheth	10-2000

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims **1, 6 - 9, 15, 20 - 23, 29, 34 - 37** are rejected under 35 U.S.C. 102(e) as being anticipated by **Bridgelall** (US Patent No. **7,039,027**)

With Regards to Claims 1, 15, 29, Bridgelall discloses a method, machine-readable storage having stored upon a computer program having at least one code section,

system for multiple encryption in a multi-band multi-protocol hybrid wired/wireless network, the method comprising:

a) receiving on a first PHY channel of an access point, a request for initiation of a communication session from an originating access device; (see Bridgelall col 6, lines 7-9: enables user to conduct communications via the network via an access point; col. 7, lines 33-36: mobile unit (wireless device) posts a request to network via channel 336)

b) authenticating said communication session by authenticating said access using a second PHY channel; (see Bridgelall col 6, lines 7-9: enables user to conduct communications via the network via an access point; col. 7, lines 39 - 66: connection management service request via dedicated channel 338 or 340; authentication center provides authentication request to mobile over dedicated channel; mobile initiates authentication response over dedicated channel; response executes a cellular authentication and voice encryption algorithm; algorithm produces a registration authentication result which is provide to service provider) and

c) hosting said communication session over a third PHY channel , said third PHY channel established between said access point and said originating access device. (see Bridgelall col 6, lines 7-9: enables user to conduct communications via the network via an access point; col. 8, lines 4-9: network assigns traffic channel for transmission of user data; assignment command from network and assignment complete message from mobile; communication on new channel

342)

With Regards to Claims 6, 20, 34, Bridgelall discloses the method, machine-readable storage having stored upon a computer program having at least one code section, system according to claims 1, 15, 29, comprising receiving an identification of said originating access device by said access point. (see Bridgelall col. 7, line 61 - col. 8, line 2: message indicates type of service, user number, and identification of the mobile (wireless device))

With Regards to Claims 7, 21, 35, Bridgelall discloses the method, machine-readable storage having stored upon a computer program having one code section, system according to claims 6, 20, 34, wherein said identity of said originating access device is one or more of a WEP key, a MAC address, and/or an IP address. (see Bridgelall col. 12, lines 29-38: communication with MAC layer; devices connected to the physical layer are under the direction of a MAC management routine (MAC address); MAC layer implies a MAC address; col 12, lines 42-46: internet protocol layer, data delivery using TCP (IP address))

With Regards to Claims 8, 22, 36, Bridgelall discloses the method, machine-readable storage having stored upon a computer program having at least one code section, system according to claims 1, 15, 29, comprising acknowledging said received request on said first PHY channel. (see Bridgelall col. 7, lines 36-39: network provides a

channel assignment via channel 334 which provides parameters for access to dedicated channel for call setup (acknowledgement))

With Regards to Claims 9, 23, 37, Bridgelall discloses the method, machine-readable storage having stored upon a computer program having at least one code section, system according to claims 1, 15, comprising determining a type of traffic generated by said originating access device on said first PHY channel. (see Bridgelall col. 7, line 67 - col 8, lines 1: call setup indicates the type of service required (type of traffic))

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims **2 - 5, 10, 11, 16 - 19, 24, 25, 30 - 33, 38, 39** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Bridgelall** in view of **He et al.** (US Patent No. **6,088,451**).

With Regards to Claims 2, 16, 30, Bridgelall discloses the method, machine-readable storage having stored upon a computer program having at least one code section according to claims 1, 15 with at least one encryption/decryption key for use during said

communication session. (see Bridgelall col. 9, lines 31-42: mobile station (wireless device) has received a key through secure channel; mobile station provides an authentication response to access point; authentication status transmitted to mobile station (wireless device))

Bridgelall does not specifically disclose generating encryption/decryption key. However, He discloses wherein further comprising generating. (see He col. 18, lines 2-5; col. 19, lines 8-11; col. 20, lines 57-61: generation encryption/decryption key)

It would have been obvious to one of ordinary skill in the art to modify Bridgelall for generation encryption/decryption key as taught by He. One of ordinary skill in the art would have been motivated to employ the teachings of He for network-wide centralized user administration and authentication, credential management and network element access. (see He col.1, lines 59-63)

With Regards to Claims 3, 17, 31 Bridgelall discloses the method, machine-readable storage having stored upon a computer program having at least one code section, system according to claims 2, 17, 31, wherein said authenticating comprises requesting authentication information from an authentication server. (see Bridgelall col 6, lines 7-9: enables user to conduct communications via the network via an access point; col. 7, lines 39 - 66: connection management service request via dedicated channel 338 or 340; authentication center provides authentication request to mobile over dedicated channel; mobile initiates authentication response over dedicated channel; response executes a cellular authentication and voice encryption algorithm; algorithm produces a

registration authentication result which is provide to service provider; (authentication center)

With Regards to Claims 4, 18, 32, Bridgelall discloses the method, machine-readable storage having stored upon a computer program having at least one code section, system according to claims 3, 17, 31, wherein said authenticating comprises delivering at least a portion of said authentication information received from said authentication server to said originating access device via said second PHY channel. (see Bridgelall col 6, lines 7-9: enables user to conduct communications via the network via an access point; col. 7, lines 39 - 66: connection management service request via dedicated channel 338 or 340; authentication center provides authentication request to mobile over dedicated channel; mobile initiates authentication response over dedicated channel; response executes a cellular authentication and voice encryption algorithm; algorithm produces a registration authentication result which is provide to service provider; dedicated channel is second PHY channel)

With Regards to Claims 5, 19, 33, Bridgelall discloses the method, machine-readable storage having stored upon a computer program having at least one code section, system according to claims 4, 18, 32, wherein comprising delivering said at least one encryption/decryption key to said originating access device via one of said first PHY channel or said second PHY channel. (see Bridgelall col. 9, lines 31-42: mobile station (wireless device) has received a key through secure channel; mobile station provides an

authentication response to access point; authentication status transmitted to mobile station (wireless device))

With Regards to Claims 10, 24, 38, Bridgelall discloses the method, machine-readable storage having stored upon a computer program having at least one code section, system according to claims 9, 23, 37, further comprising at least one key dependent on said determined traffic type. (see Bridgelall col. 9, lines 31-42: mobile station (wireless device) has received a key through secure channel; mobile station provides an authentication response to access point; authentication status transmitted to mobile station (wireless device))

Bridgelall does not specifically disclose generating encryption/decryption key. However, He discloses wherein comprising generating at least one encryption/decryption key. (see He col. 18, lines 2-5; col. 19, lines 8-11; col. 20, lines 57-61: generation encryption/decryption key)
Motivation for He to disclose generating an encryption/decryption key is as stated in Claim 2 above.

With Regards to Claims 11, 25, 39, Bridgelall discloses the method, machine-readable storage having stored upon a computer program having at least one code section, system according to claims 10, 24, 38, wherein comprising distributing said at least one encryption/decryption key via at one or both of said second PHY channel and/or said

third PHY channel. (see Bridgelall col. 9, lines 31-42: mobile station (wireless device) has received a key through secure channel; mobile station provides an authentication response to access point; authentication status transmitted to mobile station (wireless device))

He discloses generating an encryption/decryption key is as stated in Claim 2 above.

8. Claims **12 - 14, 26 - 28, 40 - 42** are rejected under 35 U.S.C. 103 (a) as being unpatentable over **Bridgelall** in view of **Sheth et al.** (US Patent No. **7,325,058**).

With Regards to Claims 12, 26, 40, Bridgelall discloses the method, machine-readable storage having stored upon a computer program having at least one code section according to claims 1, 15, 29, further comprising establishing at least one channel between said originating access device and a terminating access device. (see Bridgelall col 6, lines 7-9: enables user to conduct communications via the network via an access point; col. 7, lines 33-36: mobile unit (wireless device) posts a request to network via channel 336)

Bridgelall does not specifically disclose a virtual channel.

However, Sheth discloses establishing a virtual channel. (see Sheth col. 6, lines 62-67: virtual circuit or channel is a logical circuit for reliable communications between two network devices; virtual circuit (channel) identified by Virtual Path Identifier; col. 7, lines 19-31: limiting access to networks associated with a virtual circuit (channel); tunnel ID determined based upon domain name and virtual circuit (channel) identifier))

It would have been obvious to one of ordinary skill in the art to modify Bridgelall tfor a virtual channel as taught by Sheth. One of ordinary skill in the art would have been motivated to employ the teachings of Sheth for more secure control over which domains a particular subscriber may connect to using the widely used PPP protocol to combat intrusion such as denial of service attacks. (see Sheth col. 4, lines 24-26)

With Regards to Claims 13, 27, 41, Bridgelall discloses the method, machine-readable storage having stored upon a computer program having at least one code section, system according to claims 12, 26, 40, comprises transferring information between said originating access device and said terminating access device. (see Bridgelall col 6, lines 7-9: enables user to conduct communications via the network via an access point; col. 7, lines 39 - 66: connection management service request via dedicated channel 338 or 340; authentication center provides authentication request to mobile over dedicated channel; mobile initiates authentication response over dedicated channel; response executes a cellular authentication and voice encryption algorithm; algorithm produces a registration authentication result which is provide to service provider)

Bridgelall does not specifically disclose tunneling
However, Sheth discloses tunneling information between originating access device and terminating access device. (see Sheth col. 6, lines 62-67: virtual circuit or channel is a logical circuit for reliable communications between two network devices; virtual circuit (channel) identified by Virtual Path Identifier; col. 7, lines 19-31: limiting access to networks associated with a virtual circuit (channel); tunnel ID determined based upon

domain name and virtual circuit (channel) identifier))

Motivation for Sheth to disclose tunneling is as stated in Claim 12 above.

With Regards to Claims 14, 28, 42, Bridgelall discloses the method, machine-readable storage having stored upon a computer program having at least one code section, system according to claims 12, 26, 40, comprising establishing at least a portion of said at least one channel over at least a portion of one of said first PHY channel, said second PHY channel or said third PHY channel. (see Bridgelall col 6, lines 7-9: enables user to conduct communications via the network via an access point; col. 7, lines 33-36: mobile unit (wireless device) posts a request to network via channel 336)
Sheth discloses a virtual channel as stated in Claim 12 above.

(10) Response to Argument

3.1 Applicant argues, "receiving on a first PHY channel of an access point, a request for initiation of a communication session from an originating access device," or "authenticating said communication session by authenticating said originating access device using a second PHY channel," or "hosting said communication session over a third PHY channel, said third PHY channel established between said access point and said originating access device,". (Remarks Page 10, Lines 4-9)

Bridgelall discloses the indicated claim limitations. Bridgelall discloses a first channel utilized to transmit a request for communications; a second channel used to transmit

authentication information; and a third channel used to host communications for the mobile device after completion of authentication.

Bridgelall discloses the claim limitations for Claim 1 as follows:

Channel 336 (first PHY channel)

- receiving on a first PHY channel of an access point, a request for initiation of a communication session from an originating access device; (see Bridgelall col 6, lines 7-9: enables user to conduct communications via the network via an access point; col. 7, lines 33-36: mobile unit (wireless device) posts a request to network via channel 336)

Channel 338 (second PHY channel)

- authenticating said communication session by authenticating said access using a second PHY channel; (see Bridgelall col 6, lines 7-9: enables user to conduct communications via the network via an access point; col. 7, lines 39 - 66: connection management service request via dedicated channel 338 or 340; authentication center provides authentication request to mobile over dedicated channel; mobile initiates authentication response over dedicated channel; response executes a cellular authentication and voice encryption algorithm; algorithm produces a registration authentication result which is provide to service provider)

Channel 342 (third PHY channel)

- hosting said communication session over a third PHY channel, said third PHY channel established between said access point and said originating access

device. (see Bridgelall col 6, lines 7-9: enables user to conduct communications via the network via an access point; col. 8, lines 4-9: network assigns traffic channel for transmission of user data; assignment command from network and assignment complete message from mobile; communication on new channel 342)

Three different channels (336, 338 and 342) are utilized to perform the three separate steps of Claim 1. In other disclosures, Bridgelall discloses that an authentication process is completed between the mobile and access point. (see Bridgelall col 9, lines 17-23: authentication process between mobile unit and access point)

3.2 Applicant argues, *the originating access device (i.e., 604), the authenticating server (i.e., 612) and the terminating access device (i.e., 614) cannot directly communicate to each other, without communicating via the AP (606). (Remarks Page 10, Lines 16-18)*

Bridgelall discloses that communications for the mobile device does communicate through an access point (AP) to a network-connected mobile device (indicated as the originating access device). (see Bridgelall col 6, lines 7-10: communications with WLAN is via the access point; communications for the mobile device goes through the access point)

3.3 Applicant argues, Bridgelall simply does not disclose or suggest that any of the

alleged first, second. or third PHY channel communicates to the AP (Remarks Page 13, Lines 19-21)

Bridgelall discloses that communication for the mobile device does communicate through an access point (AP) to a network-connected mobile device. (see Bridgelall col 6, lines 7-10: communications with WLAN is via the access point; communications for the mobile device goes through the access point)

Refer to Section 3.2.

3.4 Applicant argues, "receiving on a first PHY channel of an access point, a request for initiation of a communication session from an originating access device," or "authenticating said communication session by authenticating said originating access device using a second PHY channel," or "hosting said communication session over a third PHY channel, said third PHY channel established between said access point and said originating access device,". (Remarks Page 14, Lines 1-8)

Bridgelall discloses a first channel for a request for communications; a second channel for authentication information; and a third channel to host communications.

Refer Section 3.1.

3.5 Applicant argues, "receiving on a first PHY channel of an access point, a request for initiation of a communication session from an originating access device," or "authenticating said communication session by authenticating said originating access

device using a second PHY channel," or "hosting said communication session over a third PHY channel, said third PHY channel established between said access point and said originating access device,". (Remarks Page 15, Lines 3-9)

Bridgelall discloses a first channel for a request for communications; a second channel for authentication information; and a third channel to host communications.

Refer Section 3.1.

3.6 Applicant argues, "first PHY channel", "second PHY channel" and "third PHY channel", all refer to the respective PHY channels on the access point, and not on the originating access device. (Remarks Page 15, Lines 11-13)

Bridgelall discloses that communication for the radio device does communicate through an access point (AP). (see Bridgelall col 6, lines 7-10: communications with WLAN is via the access point; communications for the mobile device goes through the access point)

Refer to Section 3.2.

3.7 Applicant argues, Bridgelall simply does not disclose or suggest any of the alleged first, second or third PHY channel communicates to the AP 202 (the alleged "AP"). (Remarks Page 17, Lines 11-13)

Bridgelall discloses that communication for the mobile device does communicate through an access point (AP). (see Bridgelall col 6, lines 7-10: communications with

WLAN is via the access point; communications for the mobile device goes through the access point)

Refer to Section 3.2.

3.8 Applicant argues, Bridgelall discloses the exact opposite, namely, the alleged "first, second and third PHY channels" being of the originating access device. (Remarks Page 18, Lines 10-11)

Bridgelall does not disclose the opposite. Bridgelall discloses that communication for the mobile device does communicate through an access point (AP). (see Bridgelall col 6, lines 7-10: communications with WLAN is via the access point; communications for the mobile device goes through the access point)

Refer to Section 3.2.

3.9 Applicant argues, "receiving on a first PHY channel of an access point, a request for initiating communication session from an originating access device,". (Remarks Page 18, Lines 17-18)

Bridgelall discloses a request for communications being received over a first channel designated as channel 336. (see Bridgelall col 6, lines 7-9: enables user to conduct communications over the network via an access point; col. 7, lines 33-36: mobile unit (wireless device) posts a request to network via channel 336)

Refer to Section 3.2.

3.10 Applicant argues, Bridgelall's AP 202 does not receive the call request via the cellular RACH channel 336 (the alleged "first PHY channel") from the radio device 242 (the alleged "originating access device"). (Remarks Page 19, Lines 17-19)

Applicant is arguing that communications is not through the access point. Bridgelall discloses that communication for the mobile device does communicate through an access point (AP). (see Bridgelall col 6, lines 7-10: communications with WLAN is via the access point; communications for the mobile device goes through the access point)

3.11 Applicant argues, "hosting said communication session over a third PHY channel, said third PHY channel established between said access point and said originating access device,". (Remarks Page 20, Lines 10-13)

Bridgelall discloses that once authentication has been completed then communications for the mobile device is transmitted over a third channel designated as channel 342. (see Bridgelall col 6, lines 7-9: enables user to conduct communications via the network via an access point; col. 8, lines 4-9: network assigns traffic channel for transmission of user data; assignment command from network and assignment complete message from mobile; communication on new channel 342)

3.12 Applicant argues, "receiving on a first PHY channel of an access point, a request for initiation of a communication session from an originating access device," or

"authenticating said communication session by authenticating said originating access device using a second PHY channel," or "hosting said communication session over a third PHY channel, said third PHY channel established between said access point and said originating access device,". (Remarks Page 20, Lines 15-20)

Bridgelall discloses a first channel for a request for communications; a second channel for authentication information; and a third channel to host communications.

Refer Section 3.1.

3.13 Applicant argues, Dependent Claims 6 - 9, 20 - 23, 34 - 37. (Remarks Page 21, Lines 4-10)

Arguments against dependent claims are answered by responses to independent claims. Bridgelall disclose receiving identification information of the mobile device utilizing an access point. (see Bridgelall col. 7, line 61 - col. 8, line 2: message indicates type of service, user number, and identification of the mobile (wireless device); col 6, lines 7-10: communications with WLAN is via the access point; communications for the mobile device goes through the access point)

3.14 Applicant argues, Dependent Claims 7 - 9, 21 - 23, 35 - 37. (Remarks Page 22, Lines 5-7)

Arguments against dependent claims are answered by responses to independent claims.

3.15 Applicant argues, Dependent Claims 2 - 5, 10, 11, 16 - 19, 24, 25, 30 - 33, 38, 39. (Remarks Page 23, Lines 12-18)

Arguments against dependent claims are answered by responses to independent claims.

3.16 Applicant argues, He, nevertheless, still does not disclose that the generated encryption/decryption key between the user and network access server is "dependent on the determined traffic type,". (Remarks Page 24, Lines 16-18)

Bridgelall disclose the type of traffic communicated. (see Bridgelall col. 7, line 67 - col 8, lines 1: call setup indicates the type of service required (type of traffic); col. 9, lines 31-42: mobile station (wireless device) has received a key through secure channel; mobile station provides an authentication response to access point; authentication status transmitted to mobile station (wireless device)) And, He discloses the generation of an encryption key. (see He col. 18, lines 2-5; col. 19, lines 8-11; col. 20, lines 57-61: generation encryption/decryption key)

3.17 Applicant argues, Sheth does not overcome the deficiencies of Bridgelall. (Remarks Page 25, Lines 10-11)

Sheth is not used to disclose the indicated claim limitation.

3.18 Conclusion:

Bridgelall discloses the indicated three separate physical channels. Bridgelall discloses the first channel (indicated as channel 336) that is used to transmit a request for communications from a mobile device. Bridgelall discloses the second channel (indicated as channel 338) to communicate authentication information for the mobile device. And, Bridgelall discloses the third channel (indicated as channel 342) that is used to host communications for the mobile device after the completion of authentication. In addition, Bridgelall discloses that communications for the mobile device to the network is via an access point.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Carlton V. Johnson/

Examiner, Art Unit 2436

Conferees:

/Eleni A Shiferaw/

Primary Examiner, Art Unit 2436

/Nasser Moazzami/

Supervisory Patent Examiner, Art Unit 2436